



Y. Hsu 1

ZWAF
2/35

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Yung-Kao Hsu
Case: 1
Serial No.: 09/460,897
Filing Date: December 14, 1999
Group: 2135
Examiner: Thanhnga B. Truong

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: *Luna M. Hamli* Date: March 21, 2005

Title: Dual-Tier Security Architecture for Inter-Domain Environments

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby appeals the final rejection dated October 19, 2004, of claims 1-21 and 41-59 of the above-identified application.

REAL PARTY IN INTEREST

The present application is currently assigned to Avaya Inc. or a subsidiary thereof. Avaya Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences.

03/25/2005 AWONDAF1 00000025 501602 09460897
01 FC:1402 500.00 DA

STATUS OF CLAIMS

The present application was filed on December 14, 1999, with claims 1-59, and claims the priority of a provisional application filed April 15, 1999. Claims 1-59 are currently pending in the application. Claims 1, 41 and 54 are the independent claims.

Each of claims 1-21 and 41-59 stands finally rejected under 35 U.S.C. §102(e) or §103(a). Claims 22-40 are indicated as containing allowable subject matter. Claims 1-21 and 41-59 are appealed.

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 41 and 54 are directed to methods for establishing a secure communication between users employing endpoints in a system including one or more security zones, with each security zone having one or more of the endpoints and a Zone Keeper. The methods generally involve what is referred to in the specification as a dual-tier security architecture, where one tier is an intra-zone tier and the other tier is an inter-zone tier. Claim 1 is directed to an arrangement which may involve an inter-zone communication between endpoints in first and second security zones having respective first and second Zone Keepers. Claim 41 is directed to an arrangement involving an intra-zone communication, with authentication of a caller by a Zone Keeper, authentication by the caller of an authorization sent by the Zone Keeper, and authentication by the callee of the authorization and a communication proposal. Claim 54 is directed to an arrangement which may involve an inter-zone communication, with a second Zone Keeper authenticating that a communication request message is from a first Zone Keeper.

An illustrative embodiment of the invention is shown in FIG. 1 of the drawings. In this embodiment, there are first and second security zones 101-1 and 101-2, having respective Zone Keepers 102-1 and 102-2. Each of the security zones includes a number of endpoints 103 arranged as shown. In this embodiment, a Zone Keeper is described as an operation, administration and maintenance facility provided by the enterprise associated with the security zone to enforce a security

policy for communication in that security zone and between that security zone and other security zones. See the specification at column 3, line 14, to column 4, line 6. Flow diagrams for intra-zone and inter-zone communications in the system of FIG. 1 are shown in FIGS. 2 and 3, respectively, and described in the corresponding text at page 6, line 4, to page 10, line 13.

The dual-tier security architecture of the illustrative embodiment provides a number of advantages over conventional methods for establishing a secure communication. For example, system scalability is improved for intra-enterprise and inter-enterprise communications. Also, individual endpoints or their associated users need not have knowledge of the security mechanism for inter-zone secure communications, and endpoints in different security zones can communicate securely as though they were in the same security zone. Thus, the illustrative embodiment considerably facilitates intra-zone and inter-zone secure communication. See the specification at, for example, page 1, lines 21-29, and page 2, lines 21-25.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-12, 15-17, 41-51 and 54-56 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,269,149 (hereinafter “Hassell”).
2. Claims 13, 14, 18-21, 52, 53 and 57-59 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hassell in view of U.S. Patent No. 6,327,660 (hereinafter “Patel”).

ARGUMENT

GROUND 1

Claims 1-3

The Manual of Patent Examining Procedure (MPEP), Eight Edition, August 2001, §2131, specifies that a given claim is anticipated “only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference,” citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the “identical invention . . . in as complete detail as is contained in the . . . claim,” citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

As noted above, the present invention is generally directed to methods for establishing secure communications between users employing endpoints in a system which includes one or more security zones each having an associated Zone Keeper. An arrangement of this type is referred to in the specification as a dual-tier security architecture. With reference to independent claim 1, this claim more particularly specifies that a first Zone Keeper, associated with a first security zone including a first endpoint, determines whether a requested secure communication, between a caller utilizing the first endpoint and a callee utilizing a second endpoint, is an intra-zone or an inter-zone communication. If the requested communication is an intra-zone communication, both the first and second endpoints are in the same security zone, and the first Zone Keeper in conjunction with the first and second endpoints in the first security zone establishes the secure communication between the caller and the callee. If the requested communication is an inter-zone communication, the first and second endpoints are in first and second security zones, respectively, the first Zone Keeper sends a request message to a second Zone Keeper associated with the second security zone, and the secure communication is established between the zones utilizing the first and second Zone Keepers and the associated first and second endpoints.

The Hassell reference relied upon by the Examiner fails to meet the above-noted limitations of independent claim 1. For example, there is no mention whatsoever in Hassell regarding the claimed security zones, each having an associated Zone Keeper, or the claimed determination as to whether a given requested secure communication constitutes an intra-zone or inter-zone communication. Thus, Hassell fails to teach or suggest a dual-tier security architecture of the type claimed.

The Examiner at page 16, lines 15-17, of the final Office Action argues that such a reference to a dual-tier security architecture “does not even address in [sic] the claim language.” As indicated above, claim 1, by way of example, includes limitations relating to intra-zone communication and inter-zone communication. Intra-zone communications are handled by a first Zone Keeper in a corresponding first security zone. Inter-zone communications, on the other hand, involve particular interactions between a first Zone Keeper associated with a first security zone and a second Zone Keeper associated with a second security zone. The specification makes clear that this type of security architecture, involving distinct handling of intra-zone communications and inter-zone

communications from a security standpoint, is referred to as a dual-tier security architecture. See the specification at, for example, page 1, lines 21-29, and page 3, lines 14-15. Accordingly, claim 1 does describe a dual-tier security architecture, by its references to distinct handling of intra-zone and inter-zone communications, and to first and second security zones and their respective first and second Zone Keepers.

In formulating the §103(a) rejection, the Examiner specifically relies on the teachings in Hassell at column 2, line 60, to column 3, line 20. This portion of the cited reference provides as follows:

In accordance with another aspect of the present invention, a method for establishing a secured telecommunications link between a calling party and a called party is provided. In accordance with this aspect of the invention, the method includes the steps of receiving a calling from a remote user, identifying the caller identification number, and using caller identification number to access a lookup table. The method further includes the steps of determining whether a profile exists in the lookup table that corresponds to the identified caller identification element. If so, the method further confirms from information provided in the lookup table, whether that user is entitled to access the system. If so, then the method directs the system to establish the connection with the remote user. In a preferred embodiment, the system may provide an added level of security by requiring the remote user to enter a password, as well.

Preferably, this aspect of the invention includes the steps of receiving a signal from a calling party that is requesting the establishment of a communication link, and examining call setup information within the received signal for the second calling party to identify the telephone number of the second calling party. The method further includes the steps of accessing a memory storage area using the telephone number of the second calling party to retrieve information relating to the calling party, and evaluating security data of the retrieved information. If the security data permits the establishment of a connection, then the method establishes a communication link with the calling party.

It is readily apparent that the relied-upon passages quoted above fail to make any reference to security zones or a determination as to whether a given communication is an intra-zone or inter-zone communication. By treating all communications in substantially the same manner, without regard to the relationship of the associated endpoints to one or more security zones, Hassell actually teaches away from the invention as recited in claim 1.

The Examiner also makes reference to column 4, lines 29-33, and to the drawing in FIG. 1 of Hassell which shows a first or calling endpoint 12 and a second or called endpoint 14 communicating over a network 16. Again, there is no teaching or suggestion here or anywhere else in Hassell regarding endpoints 12 or 14 potentially being in different security zones associated with respective Zone Keepers, nor any determination as to whether a given requested secure communication is an intra-zone communication or an inter-zone communication.

In the final Office Action, at page 15, last paragraph, to page 16, first paragraph, the Examiner relies on the teachings in column 7, lines 11-20, and column 1, lines 35-67, of Hassell. The teachings from column 7, lines 11-20, provide as follows:

Turning now to FIG. 3, a flowchart is provided that depicts the top-level operation of the prioritization aspect of the present invention. Specifically, upon receiving an incoming call, the system validates the call by way of identifying the caller ID (at step 60). This validation step, having been briefly described above, will be described in more detail in connection with FIG. 4. Upon validating the caller ID, the system then determines from an internal database (at step 62) whether it has a prioritization profile for this particular caller ID. If not, it rejects the incoming call (step 64).

The Examiner argues that the “system” referred to in this passage corresponds to one of the claimed Zone Keepers. Apparently, the “system” referred to in this passage is the system shown in FIG. 1 of Hassell, which includes calling endpoint 12, called endpoint 14, and the network 16 over which they communicate. However, there is no indication in Hassell to the effect that there are multiple such systems which interact in the manner set forth in claim 1 to establish secure inter-zone communications.

The teachings from column 1, lines 35-67, of Hassell, provide as follows:

There are, however, various shortcomings in the present state of the art, including the handling of fault detection, security, and call prioritization. Mechanisms are well known for identifying and notifying a user of a line breakage or other fault condition existing in the link between endpoints. However, endpoint equipment often responds by rerouting all data on a particular line, as opposed to on the affected data. For example, suppose one endpoint of a telecommunications network interfaces to a local area network (e.g. a corporate network) and the telecommunications link communicating with the endpoint is a high capacity T1 line. If the endpoint detects a fault or breakage in any channel(s) of the T1 line, present systems operate to reroute the entirety of the data traffic across that T1 line through another port, whether that be a secondary T1 line or an alternative backup link. However, fractional or partial line faults are often encountered, making such a global rerouting of data wasteful and unnecessary. For example, data transmitted across a frame relay network (e.g., packet-switched data) often suffers only a partial fault, or a network breakage at some intermediate point across which only a portion of the data to the ultimate endpoint traverses.

Another shortcoming noted in present state of the art systems relates to security. In keeping with the previous example of telecommunications network endpoint being connected to a local area network, there is a tremendous need for providing a secured entry from any caller outside the local area network to access the network by way of, for example, a dial-up connection. Frequently security issues, such as this one, are handled by password protection. In such systems, dial-up users are required to provide a password for access to the network.

Again, this fails to provide any teaching or suggestion regarding the separation of a system into security zones, each including a corresponding Zone Keeper, as claimed. At best, it simply indicates the well-known notion that a caller may be required to enter a password to obtain access to a local area network. This is not what Applicant is attempting to claim, as is readily apparent from even a cursory review of claim 1.

Applicant also notes that the technique that Hassell uses to provide secure communications is described generally at column 2, line 59, to column 3, line 8, which portion was previously quoted above. There is no mention in this teaching regarding the separation of a system into security zones, each with a corresponding Zone Keeper, and interaction between the Zone Keepers in the manner specified in claim 1. Accordingly, the Hassell system fails to provide the advantages of the claimed invention in terms of its ability to facilitate intra-zone and inter-zone secure communication. See the specification at, for example, page 1, lines 21-29, and page 2, lines 21-25.

Since independent claim 1 includes limitations which are not disclosed in Hassell, that reference is not anticipatory of claim 1.

Dependent claims 2 and 3 are believed allowable for at least the reasons identified above with regard to independent claim 1.

Claim 4

Dependent claim 4 calls for providing a capability by each of said Zone Keepers to have registered by users using an endpoint associated with a particular Zone Keeper individual prescribed security policies and said particular Zone Keeper enforcing said prescribed security policies. Hassell fails to disclose an arrangement in which users are permitted to register particular security policies with a Zone Keeper in a dual-tier security architecture.

Claims 5-10

Dependent claim 5 further refines the method of claim 1 by calling for the establishment of an intra-zone communication using particular steps, including:

said first Zone Keeper sending an authorization message including an authorization of said caller communication request to said caller, via said first endpoint, said authorization including security information identifying said first Zone Keeper and security information identifying said callee;

said caller authenticating the authorization sent by said first Zone Keeper;

said caller sending, via said first endpoint, a connection request message including a communication proposal for establishing a multimedia communication connection with said callee, via said second endpoint;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that said callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints in said first security zone, wherein a secure multimedia communication is established.

It is respectfully submitted that this particular protocol is not taught or suggested by the relied-upon portions of the Hassell reference. Also, Hassell is believed to teach away from the particular arrangement claimed by teaching to use other arrangements that fail to provide the advantages associated with the claimed arrangement.

Dependent claims 6-10 are believed allowable for at least the reasons identified above with regard to dependent claim 5.

Claim 11

Dependent claim 11 further refines the method of claim 5 by calling for a connection request message having a particular format, namely, one which includes an authorization from a Zone Keeper, security information identifying the caller to the callee, and a communication proposal of how the secure caller-callee communication connection is to be set-up. There is no connection request message disclosed in Hassell which has this particular format.

Claim 12

Dependent claim 12 further limits the connection request message format by specifying that the connection request message includes security information for authenticating the identity of the callee. The Examiner relies on column 5, lines 63-67, of Hassell, but this portion of the reference

does not disclose any type of connection request message format, much less the particular one recited in the claim.

Claims 15-17

Dependent claim 15 further defines the manner in which the inter-zone communication referred to in claim 1 is established. The recited communication protocol includes the following limitations:

said first Zone Keeper forwarding said communication request message to a second Zone Keeper associated with said second security zone;

said second Zone Keeper authenticating that the communication request message is from said first Zone Keeper;

said second Zone Keeper sending an authorization message including an authorization of said caller communication request to said first Zone Keeper, said authorization message including security information identifying said second Zone Keeper and security information identifying said callee;

said first Zone Keeper authenticating the authorization in said authorization message sent by said second Zone Keeper;

if said authorization in said authorization message is authenticated, said first Zone keeper sending said authorization message to said caller via said first endpoint;

said caller sending, via said first endpoint, a connection request message including a communication proposal for establishing a secure multimedia communication connection with said callee, via said second endpoint;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints, wherein a secure multimedia communication is established.

The Examiner argues that each and every one of these limitations is disclosed in Hassell. However, Applicant has studied the portions of the reference relied upon by the Examiner, and respectfully disagrees. The claim sets forth a particular communication protocol implemented in a dual-tier security architecture arrangement, and is not taught or suggested by Hassell.

Dependent claims 16 and 17 are believed allowable for at least the reasons identified above with regard to dependent claim 15.

Claims 41-46

Independent claim 41 is directed to a dual-tier security architecture arrangement involving an intra-zone communication, and recites, among other elements, authentication of a caller by a Zone Keeper, authentication by the caller of an authorization sent by the Zone Keeper, and authentication by the callee of the authorization and a communication proposal.

Applicant submits that Hassell fails to teach or suggest the security zone, Zone Keeper and communication protocol limitations of independent claim 41, and in fact teaches away from the claimed arrangement by teaching to use arrangements different than those specifically claimed in order to set up a secure communication between endpoints.

Dependent claims 42-46 are believed allowable for at least the reasons identified above with regard to independent claim 41.

Claim 47-51

Dependent claim 47 calls for a particular connection request message format, namely, one which includes an authorization from a Zone Keeper, security information identifying a caller to a callee, and a communication proposal of how the secure caller-callee communication connection is to be set-up. The Examiner relies on the rationale used to reject claim 11, but again, Applicant has been unable to find in Hassell any disclosure that is anticipatory of the particular format limitation in question.

Dependent claims 48-51 are believed allowable for at least the reasons identified above with regard to dependent claim 47.

Claims 54-56

Independent claim 54 is directed to a dual-tier security architecture arrangement which may involve an inter-zone communication, and recites, among other limitations, a second Zone Keeper authenticating that a communication request message is from a first Zone Keeper.

Applicant submits that Hassell fails to teach or suggest the security zone, Zone Keeper and communication protocol limitations of independent claim 54, and in fact teaches away from the claimed arrangement by teaching to use arrangements different than those specifically claimed in order to set up a secure communication between endpoints.

Dependent claims 55 and 56 are believed allowable for at least the reasons identified above with regard to independent claim 54.

GROUND 2

Claims 13 and 14

Dependent claim 13 calls for a first Zone Keeper providing authentication of its identity by using public-key cryptography and a digital signature, and user authentication of the first Zone Keeper identity by employing said first Zone Keeper's public key. The proposed combination of Hassell and Patel fails to teach or suggest a dual-tier architecture in which a Zone Keeper provides authentication of its identity in the particular manner claimed.

A proper *prima facie* case of obviousness requires that the cited references when combined must "teach or suggest all the claim limitations," and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references or to modify the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

The Patel reference cited by the Examiner fails to overcome the fundamental deficiencies of Hassell as applied to the independent claims. Thus, the proposed combination fails to "teach or suggest all the claim limitations" as is required for establishment of a proper *prima facie* case.

Furthermore, the Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination “must be based on objective evidence of record” and that “this precedent has been reinforced in myriad decisions, and cannot be dispensed with.” In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). The Federal Circuit has further stated that “conclusory statements” by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved “on subjective belief and unknown authority.” Id. at 1343-1344. Applicant submits that the Examiner has failed to provide any objective evidence of motivation to combine Hassell and Patel, or to modify their teachings, to meet the claim limitations in question. The particular statement provided by the Examiner is on page 14, last paragraph, to page 15, first paragraph, of the final Office Action, and is as follows:

The ordinary skilled person would have been motivated to add such security association 700 (in Hassell) because a communication channel is considered to be “secure” when (i) the modification of data transmitted through the communication channel can be detected, and (ii) the source of the transmitted data can be authenticated, and/or the confidentiality of the transmitted data is protected. Cryptographic techniques such as digital certificates, digital signatures, and the encryption/decryption of data are used to secure a communication channel.

There is no objective evidence of motivation here. The Examiner has instead provided only a conclusory statement of obviousness based on the type of “subjective belief and unknown authority” that the Federal Circuit has indicated is insufficient to support an obviousness rejection. At best, the quoted statement simply indicates the well-known fact that cryptographic techniques can be used to provide secure communication. This alone is insufficient evidence of motivation to combine the particular cryptographic techniques of Patel, which are specifically designed for use in a “pre-boot environment,” that is, for use prior to booting of an operating system, with the communication processing techniques of Hassell. In a sense, Hassell and Patel are non-analogous because Hassell bears no relation to the pre-boot environment while Patel is specifically directed to that context. Accordingly, additional objective motivation to combine Hassell and Patel is required to support a

prima facie case of obviousness, beyond the mere notion that cryptographic techniques can be used to provide secure communication.

Dependent claim 14 is believed allowable for at least the reasons identified above with regard to dependent claim 13.

Claims 18-20

Dependent claim 18 calls for each of a plurality of Zone Keepers having its own private key, and further specifies that a first Zone Keeper signs a communication request message, so as to permit authentication of the message by a second Zone Keeper, through said first Zone Keeper's private key. The proposed combination of Hassell and Patel fails to disclose a dual-tier security arrangement with first and second Zone Keepers operating as claimed.

Dependent claims 19 and 20 are believed allowable for at least the reasons identified above with regard to dependent claim 18.

Claim 21

Dependent claim 21 calls for each of the users recited in claim 1 having its own password which is registered by the user of an endpoint with the endpoint's associated Zone Keeper, and each of said Zone Keepers having its own private key and its own public key. The claim further specifies that a communication request message includes a first prescribed security token, with the first Zone Keeper authenticating the first prescribed security token, and if the first prescribed security token is authenticated, determining that said communication should be allowed. However, the combined teachings of Hassell and Patel fail to meet the particular communication protocol steps recited in the claim. The Examiner relies on general cryptographic functionality recited in Patel, but fails to indicate how one skilled in the art would be motivated to modify such general functionality to meet the particular limitations recited in the claim. Again, the proposed combination also fails to meet the dual-tier security architecture aspects of the claim.

Claims 52 and 53

Dependent claims 52 and 53 are believed allowable for at least the reasons identified above with regard to claim 47.

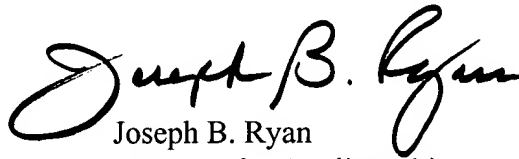
Claims 57-59

Dependent claim 57 includes limitations similar to those of claim 18, but depends from claim 54 rather than claim 1. Again, it is believed that the proposed combination of Hassell and Patel fails to disclose a dual-tier security arrangement with first and second Zone Keepers operating in the particular manner claimed.

Dependent claims 58 and 59 are believed allowable for at least the reasons identified above with regard to claim 57.

In view of the above, Applicant believes that claims 1-59 are in condition for allowance, and respectfully requests the withdrawal of the §102(e) and §103(a) rejections.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Joseph B. Ryan". The signature is fluid and cursive, with the first name "Joseph" and last name "Ryan" clearly distinguishable.

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

Date: March 21, 2005

CLAIMS APPENDIX

1. A method for establishing a secure communication between users employing endpoints in a system including one or more security zones, each security zone including one or more of said endpoints and a Zone Keeper, wherein at least one of said users is a caller utilizing a first endpoint in one of said one or more security zones and at least another one of said users is a callee utilizing a second endpoint in one of said one or more security zones, the method including the steps of:

said caller sending a communication request message including a communication request for establishing a secure multimedia communication including security information identifying said caller, via said first endpoint to a first one of said Zone Keepers associated with a security zone including said first endpoint;

said first Zone Keeper authenticating the identity of said caller, and if said caller identity is authenticated, authorizing said caller's communication request;

said first Zone keeper determining whether said requested secure communication is an intra-zone or an inter-zone communication:

if said requested communication is an intra-zone communication both said first and second endpoints are in the same security zone, said first Zone Keeper in conjunction with said first and second endpoints in said first security zone establishing said secure communication between said caller and said callee;

if said requested communication is an inter-zone communication said first and second endpoints are in first and second security zones, respectively, said first Zone Keeper sending said request message to said second Zone Keeper associated with said second security zone; and

establishing said secure inter-zone communication utilizing said first Zone Keeper, said first endpoint in said first security zone, said second Zone Keeper and said second endpoint in said second security zone.

2. The method as defined in claim 1 further including providing a capability by each of said Zone Keepers for users of an endpoint in a security zone associated with a particular Zone Keeper to register authentication keys and/or methods and said particular Zone Keeper authenticating said users only through said registered keys and/or methods to honor requests for secure communication.

3. The method as defined in claim 1 further including providing a capability by each of said Zone Keepers to have registered authentication keys and/or methods of endpoints in a security zone associated with a particular Zone Keeper and said particular Zone Keeper authenticating only users authenticated by said user authentication keys and/or methods and said endpoint authentication keys and/or methods to honor requests for secure communication.

4. The invention as defined in claim 1 further including providing a capability by each of said Zone Keepers to have registered by users using an endpoint associated with a particular Zone Keeper individual prescribed security policies and said particular Zone Keeper enforcing said prescribed security policies.

5. The method as defined in claim 1 wherein said intra-zone communication is established by the further steps of

said first Zone Keeper sending an authorization message including an authorization of said caller communication request to said caller, via said first endpoint, said authorization including security information identifying said first Zone Keeper and security information identifying said callee;

said caller authenticating the authorization sent by said first Zone Keeper;

said caller sending, via said first endpoint, a connection request message including a communication proposal for establishing a multimedia communication connection with said callee, via said second endpoint;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that said callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints in said first security zone, wherein a secure multimedia communication is established.

6. The method as defined in claim 5 further including, if said first Zone Keeper rejects said communication request from said caller, said first Zone Keeper sending an authorization rejected message indicating that said communication request was rejected to said caller, via said first endpoint.

7. The method as defined in claim 5 wherein said connection request message includes said communication authorization and security information for authenticating the identity of said callee.

8. The method as defined in claim 7 wherein said connection message further includes a proposal indicating how the caller-callee communication should be set-up.

9. The method as defined in claim 5 further including said first Zone Keeper employing a prescribed security arrangement for authenticating the identity of said caller.

10. The method as defined in claim 9 wherein said prescribed security arrangement includes using a caller identification (ID) and corresponding password.

11. The method as defined in claim 5 wherein said connection request message includes said authorization from said Zone Keeper, security information identifying said caller to said callee and a communication proposal of how the secure caller-callee communication connection is to be set-up.

12. The method as defined in claim 11 wherein said connection request message further includes security information for authenticating the identity of said callee.

13. The invention as defined in claim 11 further including said first Zone Keeper providing authentication of its identity by using public-key cryptography and a digital signature and wherein

said users authenticate the first Zone Keeper identity by employing said first Zone Keeper's public key.

14. The invention as defined in claim 13 further obtaining said digital signature by said first Zone Keeper signing said request response message with a private-key.

15. The method as defined in claim 1 wherein said inter-zone communication is established by the further steps of

said first Zone Keeper forwarding said communication request message to a second Zone Keeper associated with said second security zone;

said second Zone Keeper authenticating that the communication request message is from said first Zone Keeper;

said second Zone Keeper sending an authorization message including an authorization of said caller communication request to said first Zone Keeper, said authorization message including security information identifying said second Zone Keeper and security information identifying said callee;

said first Zone Keeper authenticating the authorization in said authorization message sent by said second Zone Keeper;

if said authorization in said authorization message is authenticated, said first Zone keeper sending said authorization message to said caller via said first endpoint;

said caller sending, via said first endpoint, a connection request message including a communication proposal for establishing a secure multimedia communication connection with said callee, via said second endpoint;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints, wherein a secure multimedia communication is established.

16. The method as defined in claim 15 further including, if said first Zone Keeper rejects said communication request from said caller, said first Zone Keeper sending an authorization rejected message indicating that said communication request was rejected to said caller, via said first endpoint.

17. The method as defined in claim 15 further including said first Zone Keeper determining whether said caller and said callee are security compatible for the requested secure multimedia communication.

18. The method as defined in claim 17 wherein each of said Zone Keepers has its own private key, and further including said first Zone Keeper signing said communication request message and said second Zone Keeper authenticating that said communication request message was sent by said first Zone Keeper through said first Zone Keeper's private key.

19. The method as defined in claim 18 wherein each of said Zone Keepers has its own digital signature, and further including security information indicating the identity of said callee and said second Zone Keeper including its digital signature in said authorization message sent to said first Zone Keeper, and said first Zone Keeper authenticating the authorization sent by said second Zone Keeper through the digital signature of said second Zone Keeper.

20. The method as defined in claim 19 wherein each of said Zone keepers has its own public key, said caller authenticates said authorization by verifying said digital signature of said first Zone Keeper and said callee authenticates said authorization and communication proposal by verifying the digital signature of said second Zone Keeper through its public key.

21. The method as defined in claim 1 wherein each of said users has its own password which is registered by the user of an endpoint with the endpoint's associated Zone Keeper, and each of said Zone Keepers has its own private key and its own public key and further including said communication request message including a first prescribed security token, said first Zone Keeper authenticating said first prescribed security token, and if said first prescribed security token is authenticated, determining that said communication should be allowed.

22. The method as defined in claim 21 wherein said intra-zone communication is established by the further steps of

said first Zone Keeper generating a second prescribed security token and a third prescribed security token, inserting said second and third prescribed security tokens in an authentication message and sending said authorization message to said first endpoint, said third prescribed security token including a prescribed challenge value;

said first endpoint authenticating said second prescribed security token in said authorization message and extracting said third prescribed security token;

said first endpoint sending a communication set-up message including said third prescribed security token to said second endpoint;

said second endpoint authenticating said third prescribed security token in said set-up message;

said second endpoint extracting said challenge value from said third prescribed security token and generating a response;

generating a fourth prescribed security token including said response;

said second endpoint sending a call proceeding message including said fourth prescribed security token to said first endpoint;

said first endpoint authenticating said fourth prescribed security token to authenticate said second endpoint; and

if said second endpoint is authenticated, establishing said secure multimedia communication using said first and second endpoints.

23. The method as defined in claim 22 wherein said first prescribed security token is authenticated by employing the password registered by said user of said first endpoint.

24. The method as defined in claim 23 wherein said second and third prescribed security tokens are generated using said Zone Keeper's private-key.

25. The method as defined in claim 24 wherein said second prescribed security token is authenticated by said first endpoint using said Zone Keeper's public-key.

26. The method as defined in claim 25 wherein said third prescribed security token is authenticated by said second endpoint using said Zone Keeper's public-key.

27. The method as defined in claim 26 wherein said response is generated using said registered password of said user of said second endpoint.

28. The method as defined in claim 27 wherein said first prescribed security token is an EPPwdHash security token, said second prescribed security token is a ZKIdenSign security token, said third prescribed security token is a ZKAuthorize security token and said fourth prescribed security token is an EPHashResp security token.

29. The method as defined in claim 21 wherein said inter-zone communication is established by the further steps of

said first Zone Keeper generating a second prescribed security token and including it in a second communication request message;

said first Zone Keeper sending said second communication request message to said second Zone keeper;

said second Zone Keeper determining that said second communication request message from a different security zone than the security zone including said second Zone Keeper, authenticates said second prescribed security token;

if said second Zone Keeper authorizes said communication request in said second communication request message, said second Zone Keeper generating a third prescribed security token and a fourth prescribed security token;

said second Zone Keeper generating a second communication authorization message including said third and fourth prescribed security tokens and sending said second communication authorization message to said first Zone Keeper;

said first Zone Keeper authenticating said fourth prescribed security token and if authenticated generating a fifth prescribed security token and replaces it for said fourth prescribed security token in said second communication authorization message to generate a modified second authorization communication message, and sending said modified second authorization communication message to said first endpoint;

said first endpoint authenticating said fifth prescribed security token in said modified second communication request message;

if said fifth prescribed security token is authenticated, said first endpoint generating a communication set-up message including a sixth prescribed security token including a prescribed challenge value and sending said communication set-up message to said second endpoint;

said second endpoint authenticating said sixth prescribed security token, extracting said prescribed challenge value and generating a response;

generating a seventh prescribed security token including said response;

said second endpoint generating and sending a call proceeding message including said seventh prescribed security token to said first endpoint;

said first endpoint authenticating said responses in said fifth and seventh prescribed security tokens to authenticate said second endpoint; and

if said second endpoint is authenticated, establishing said secure multimedia communication using said first and second endpoints.

30. The method as defined in claim 29 wherein said first prescribed security token is authenticated by employing the password registered by said user of said first endpoint.

31. The method as defined in claim 30 wherein said second prescribed security token is generated using said first Zone Keeper's private-key.

32. The method as defined in claim 31 wherein said second prescribed security token is authenticated by said second Zone Keeper using said first Zone Keeper's public-key.

33. The method as defined in claim 32 wherein said third prescribed security token is generated by said second Zone Keeper using said second Zone Keeper's private-key.

34. The method as defined in claim 33 wherein said fourth prescribed security token is generated by said second Zone Keeper using said second Zone Keeper's private-key.

35. The method as defined in claim 34 wherein said first Zone Keeper authenticates said fourth prescribed security token using said second Zone Keeper's public-key.

36. The method as defined in claim 35 wherein said first Zone Keeper generates said fifth prescribed security token using said first Zone Keeper's private-key.

37. The method as defined as defined in claim 36 wherein said fifth prescribed security token is authenticated by said first endpoint using said first Zone Keeper's public-key.

38. The method as defined in claim 37 wherein said sixth prescribed security token is authenticated by said second endpoint using said second Zone Keeper's public-key.

39. The method as defined in claim 38 wherein said response is generated using said registered password of said user of said second endpoint.

40. The method as defined in claim 39 wherein said first prescribed security token is an EPPwdHash security token, said second prescribed security token is a ZKZKIden security token, said third prescribed security token is a ZKAuthorize security token, said fourth prescribed security token is a second ZKZKIden security token, said fifth prescribed security token is a ZKIdenSign security token, said sixth prescribed security token is a second ZKAuthorize security token and said seventh prescribed security token is an EPHashResp security token.

41. A method for establishing a secure communication between users employing endpoints in a security zone including a plurality of said endpoints and a Zone Keeper, wherein at least one of said users is a caller utilizing an associated one of said endpoints in said security zone and at least another one of said users is a callee utilizing an associated another of said endpoints in said security zone, the method including the steps of:

said at least one caller sending a communication request message including a communication request for establishing a multimedia communication including security information identifying said caller, via said associated one of said endpoints to said Zone Keeper;

said Zone Keeper authenticating the identity of said caller, and if said caller identity is authenticated, authorizing said caller's communication request;

said Zone Keeper sending an authorization message including an authorization of said caller communication request to said caller, via said associated one of said endpoints, said authorization including security information identifying said Zone Keeper and security information identifying said callee;

said caller authenticating the authorization sent by said Zone Keeper;

said caller sending, via said associated one of said endpoints, a connection request message including a communication proposal for establishing a multimedia communication connection with said callee, via said associated another of said endpoints;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said associated another of said endpoints, to said caller via said associated one of said endpoints, an acceptance message indicating that callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said associated one of said endpoints and said associated another of said endpoints, wherein a secure multimedia communication is established.

42. The method as defined in claim 41 further including, if said Zone Keeper rejects said communication request from said caller, said Zone Keeper sending an authorization rejected message indicating that said communication request was rejected to said caller, via said associated one of said endpoints.

43. The method as defined in claim 41 wherein said connection request message includes said communication authorization and security information for authenticating the identity of said callee.

44. The method as defined in claim 43 wherein said connection message further includes a proposal indicating how the caller-callee communication should be set-up.

45. The method as defined in claim 41 further including said Zone Keeper employing a prescribed security arrangement for authenticating the identity of said caller.

46. The method as defined in claim 45 wherein said prescribed security arrangement includes using a caller identification (ID) and corresponding password.

47. The method as defined in claim 41 wherein said connection request message includes said authorization from said Zone Keeper, security information identifying said caller to said callee and a communication proposal of how the secure caller-callee communication connection is to be set-up.

48. The method as defined in claim 47 wherein said connection request message further includes security information for authenticating the identity of said callee.

49. The method as defined in claim 48 further including providing a capability by said Zone Keeper for users of an endpoint in said security zone to register authentication keys and/or methods and said Zone Keeper authenticating said users only through said registered keys and/or methods to honor requests for secure communication.

50. The method as defined in claim 49 further including providing a capability by said Zone Keeper to have registered authentication keys and/or methods of endpoints in said security zone and said Zone Keeper authenticating only users authenticated by said user authentication keys and/or

methods and said endpoint authentication keys and/or methods to honor requests for secure communication.

51. The invention as defined in claim 47 further including providing a capability by said Zone Keeper to have registered by users individual prescribed security policies and said Zone Keeper enforcing said prescribed security policies.

52. The invention as defined in claim 47 further including said Zone Keeper providing authentication of its identity by using public-key cryptography and a digital signature and wherein said users authenticate the Zone Keeper identity by employing said Zone Keeper's public key.

53. The invention as defined in claim 52 further obtaining said digital signature by said Zone Keeper signing said request response message with a private-key.

54. A method for establishing a secure communication between users employing endpoints in a system including one or more security zones, each security zone including one or more of said endpoints and a Zone Keeper, wherein at least one of said users is a caller utilizing a first endpoint in one of said one or more security zones and at least another one of said users is a callee utilizing a second endpoint in one of said one or more security zones, the method including the steps of:

said caller sending a communication request message including a communication request for establishing a secure multimedia communication including security information identifying said

caller, via said first endpoint to a first one of said Zone Keepers associated with a security zone including said first endpoint;

said first Zone Keeper authenticating the identity of said caller, and if said caller identity is authenticated, authorizing said caller's communication request;

said first Zone keeper determining whether said endpoint being used by said callee is in said first security zone or in a second one of said security zones;

if it is determined that said second endpoint in said second security, said first Zone Keeper forwarding said communication request message to a second Zone Keeper associated with said second security zone;

said second Zone Keeper authenticating that the communication request message is from said first Zone Keeper;

said second Zone Keeper sending an authorization message including an authorization of said caller communication request to said first Zone Keeper, said authorization message including security information identifying said second Zone Keeper and security information identifying said callee;

said first Zone Keeper authenticating the authorization in said authorization message sent by
said second Zone Keeper;

if said authorization in said authorization message is authenticated, said first Zone keeper
sending said authorization message to said caller via said first endpoint;

said caller sending, via said associated one of said endpoints, a connection request message including a communication proposal for establishing a secure multimedia communication connection with said callee, via said second endpoint;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints, wherein a secure multimedia communication is established.

55. The method as defined in claim 54 further including, if said first Zone Keeper rejects said communication request from said caller, said first Zone Keeper sending an authorization rejected message indicating that said communication request was rejected to said caller, via said first endpoint.

56. The method as defined in claim 54 further including said first Zone Keeper determining whether said caller and said callee are security compatible for the requested secure multimedia communication.

57. The method as defined in claim 56 wherein each of said Zone Keepers has its own private key, and further including said first Zone Keeper signing said communication request message and said second Zone Keeper authenticating that said communication request message was sent by said first Zone Keeper through said first Zone Keeper's private key.

58. The method as defined in claim 57 wherein each of said Zone Keepers has its own digital signature, and further including security information indicating the identity of said callee and said second Zone Keeper including its digital signature in said authorization message sent to said first Zone Keeper, and said first Zone Keeper authenticating the authorization sent by said second Zone Keeper through the digital signature of said second Zone Keeper.

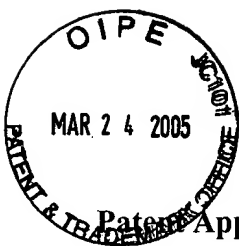
59. The method as defined in claim 58 wherein each of said Zone keepers has its own public key, said caller authenticates said authorization by verifying said digital signature of said first Zone Keeper and said callee authenticates said authorization and communication proposal by verifying the digital signature of said second Zone Keeper through its public key.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): Yung-Kao Hsu
Case: 1
Serial No.: 09/460,897
Filing Date: December 14, 1999
Group: 2135
Examiner: Thanhnga B. Truong

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: Yung-Kao Hsu Date: March 21, 2005

Title: Dual-Tier Security Architecture for Inter-Domain Environments

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith are the following documents relating to the above-identified patent application:

- (1) Appeal Brief; and
- (2) Copy of Notice of Appeal, filed on January 19, 2005, with copy of stamped return postcard indicating receipt of Notice by PTO on January 21, 2005.

There is an additional fee of \$500 due in conjunction with this submission under 37 CFR §1.17(c). Please charge **Avaya Inc. Deposit Account No. 50-1602** the amount of \$500, to cover this fee. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 50-1602** as required to correct the error. A duplicate copy of this letter is enclosed.

Respectfully submitted,

Date: March 21, 2005

Joseph B. Ryan
Reg. No. 37,922
Attorney for Applicant(s)
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

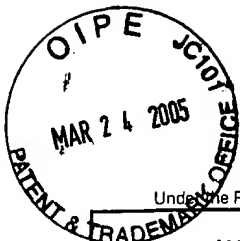


Receipt in the USPTO is hereby acknowledged of:

Transmittal Letter - 1 page
Response to Final Office Action - 8 pages
Notice of Appeal - (Orig. & 1 copy)
Revocation of Power of Attorney with New Power of Attorney
and Change of Correspondence Address - 1 page
Statement Under 37 CFR 3.73(b) - 1 page

January 19, 2005
Y. Hsu 1
Serial No. 09/460,897
1250-1092





Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PTO/SB/31 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

**NOTICE OF APPEAL FROM THE EXAMINER TO
THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Docket Number (Optional)

Y. Hsu I

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on January 19, 2005

Signature

Lisa L. Vulpis

Typed or printed
name

Lisa L. Vulpis

In re Application of
Yung-Kao Hsu

Application Number
09/460,897

Filed

December 14, 1999

For **Dual-Tier Security Architecture for Inter-Domain
Environments**

Art Unit

2135

Examiner

Thanhnga B. Truong

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1))

\$ 500.00

☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is:

\$ _____

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account. I have enclosed a duplicate copy of this sheet.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-0762. I have enclosed a duplicate copy of this sheet.

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☒ attorney or agent of record.

Registration number

37,922

Signature

Joseph B. Ryan
Joseph B. Ryan

Typed or printed name

516-759-7517

Telephone number

☐ attorney or agent acting under 37 CFR 1.34.

Registration number if acting under 37 CFR 1.34. _____

January 19, 2005

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.